

## Capítulo III

# Manejo de Incidentes

## **Manejo de Incidentes**

### **Tabla de contenido**

1.- ¿En qué consiste el manejo de incidentes? .....	45
1.1.- Ventajas .....	47
1.2.- Barreras .....	47
2.- Requerimientos .....	48
3.- Clasificación de los incidentes .....	48
4.- Escalamiento y soporte .....	49
5.- Actividades .....	50
5.1.- Registro de incidentes .....	50
5.2.- Clasificación de los incidentes .....	51
5.3.- Análisis, Resolución y Cierre de Incidentes .....	52
6.- Evaluación de la disciplina .....	53

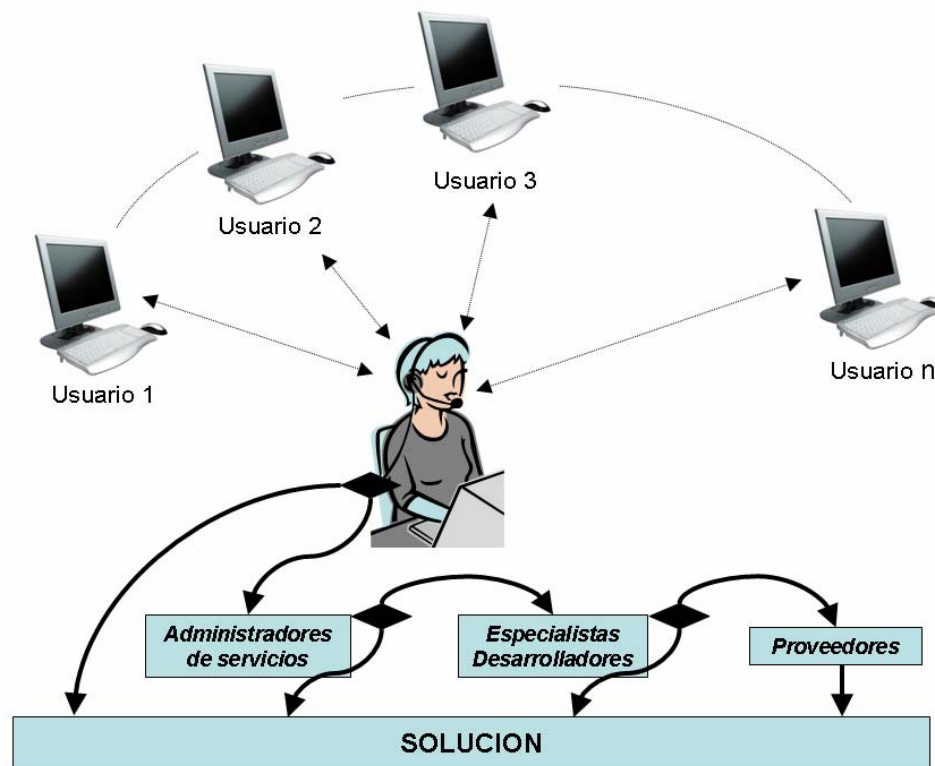
# Manejo de Incidentes

---

## 1.- ¿En qué consiste el manejo de incidentes?

Un incidente es cualquier interrupción no planeada de cualquier servicio de TI y la disciplina de manejo de incidentes busca restaurar ese servicio de la manera más rápida y eficaz posible.

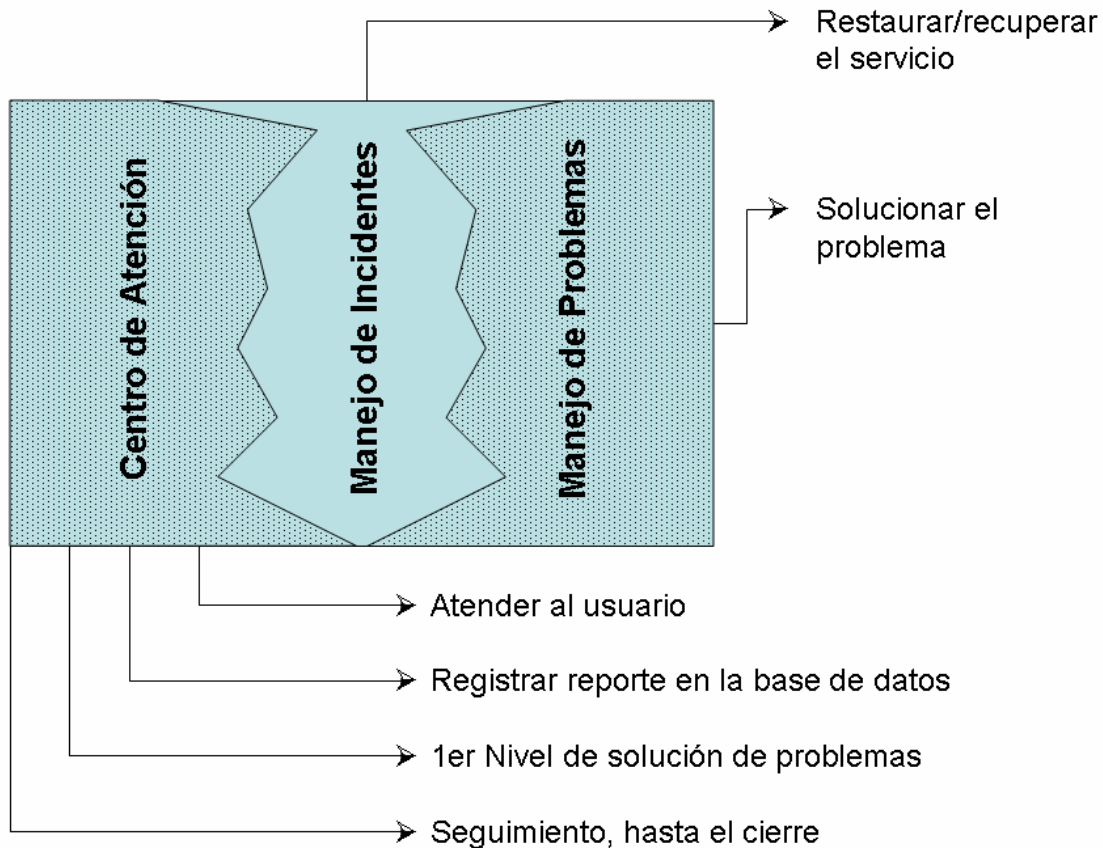
El manejo de incidentes guarda una estrecha relación con la disciplina de manejo de problemas, pero a diferencia de ésta, no se ocupa de analizar e identificar las causas que puedan haber causado un determinado incidente, sino que, como ya apuntáramos, centra su atención exclusivamente en restaurar el servicio. Es claro, sin embargo, que si bien son diferentes, guardan una estrecha interrelación.



En líneas generales, los objetivos del manejo de incidentes son:

- Detectar cualquiera alteración en los servicios TI.
- Registrar y clasificar esas alteraciones.
- Asignar el personal encargado de restaurar el servicio.

Es importante destacar que el cumplimiento de las actividades de esta disciplina requiere un estrecho contacto con los usuarios, por lo que la coordinación con el centro de atención juega un papel esencial en su desarrollo.



Normalmente, el concepto de incidente se asocia con algún funcionamiento inadecuado de los componentes de hardware o software; sin embargo, en ITIL se define como un incidente a “*Cualquier evento que no forma parte de la operación estándar de un servicio y que causa, o puede causar, una interrupción o una reducción de calidad del mismo*”.

Casi cualquier llamada que recibe el centro de atención puede clasificarse como un incidente, incluyendo las solicitudes de servicio tales como mudanza de equipos, solicitud de nuevas licencias, etc.

siempre que la solicitud corresponda a uno de los servicios que se consideren estándar de la organización.

Cualquier cambio que deba ser aplicado en cualquier elemento de de la infraestructura de TI requiere la elaboración de una solicitud de cambio que deberá ser tratada según los procedimientos de la administración de cambios.

### ***1.1.- Ventajas***

Las principales ventajas de una adecuada implementación de la disciplina de manejo de incidentes son:

- Se mejora la productividad de los usuarios.
- Se vela por el cumplimiento de los niveles de servicio acordados con los usuarios.
- Se optimiza la utilización de los recursos disponibles.
- Se dispone de una base de datos de incidentes precisa, con los incidentes relacionados a cada uno de los componentes de la infraestructura.
- Se puede lograr una mayor satisfacción de los usuarios y clientes.

Por el contrario, la carencia de un adecuado manejo de incidentes puede significar:

- Un deterioro de los niveles de servicio.
- Utilización ineficiente de los recursos.
- Pérdida de información valiosa información sobre las causas y efectos de los incidentes para poder mejorar la infraestructura de TI.
- Proliferación de clientes y usuarios insatisfechos por la mala y/o lenta atención de sus incidentes.

### ***1.2.- Barreras***

Entre las principales barreras con que tropieza la implantación de una disciplina manejo de incidentes pueden citarse las siguientes:

- No se siguen los procedimientos previstos.
- Se resuelven los incidentes sin registrarlos adecuadamente.
- Los incidentes se escalan innecesariamente.
- No están bien definidos los niveles de calidad de servicio ni los productos soportados, lo que puede provocar que se atiendan

incidentes que no corresponden a los servicios estándar o que no han sido acordados previamente con el cliente.

## ***2.- Requerimientos***

El manejo de incidentes requiere de una infraestructura que facilite su correcta implementación. Entre los elementos necesarios cabe destacar los siguientes:

- El sistema de registro de incidentes, para ser compartido con la disciplina de centro de atención.
- Una base de conocimiento, que permita comparar los nuevos incidentes que se reportan, con incidentes ya resueltos en el pasado, con el fin de:
  - Evitar transferir innecesariamente los incidentes que se reciban.
  - Convertir el conocimiento –know how- de los técnicos en un activo duradero para la empresa.
  - Poner directamente a disposición del cliente parte o la totalidad de estos conocimientos en forma de “preguntas frecuentes” –FAQs- en la intranet para los usuarios internos de la empresa o en la extranet para los clientes, con el fin de que en algunas oportunidades sea el propio usuario quien aplique el correctivo, sin necesidad de notificar el incidente.
- Una base de datos del hardware y software instalado, que permita conocer todas las configuraciones actuales y el impacto que éstas puedan tener en la resolución del incidente.

## ***3.- Clasificación de los incidentes***

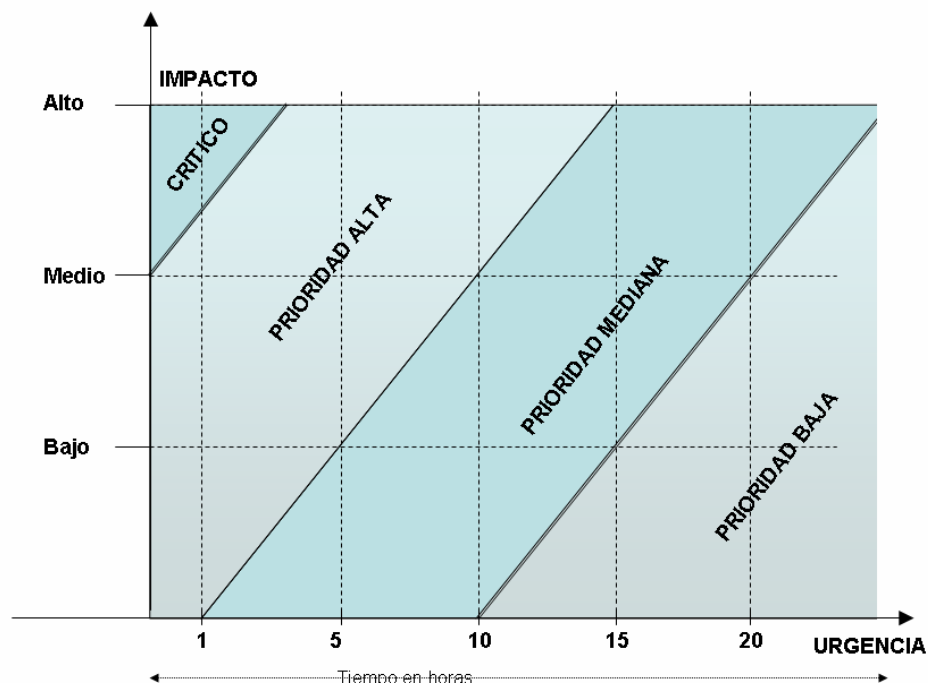
Es frecuente que se presenten múltiples incidentes concurrentemente, por lo que es necesario determinar la prioridad para atender la resolución de los mismos y asignar los recursos para atender los incidentes de mayor prioridad. El nivel de prioridad debe basarse en dos parámetros esenciales:

- Impacto  
El impacto de un incidente está determinado por la forma cómo éste afecta los procesos de negocio o por la cantidad de usuarios afectados.
- Urgencia

La urgencia de un incidente depende del tiempo máximo de que el usuario o el cliente puede esperar para la resolución del incidente, sin que la operación de su área del negocio sufra consecuencias importantes. La urgencia también depende de los niveles de servicio que hayan sido acordados con el usuario o cliente.

Para la clasificación de un incidente, además de los parámetros arriba citados, también se hace necesario tomar en cuenta factores como el tiempo de resolución esperado y los recursos necesarios para atender el incidente. Así pues, aunque en algunos casos no sean de mayor prioridad, los incidentes “sencillos” se tramitarán cuanto antes.

Es conveniente establecer criterios claros para establecer, en primera instancia, la prioridad del incidente; el “diagrama de prioridades” que se muestra en la gráfica es un ejemplo de cómo pueden establecerse esos criterios.



#### 4.- Escalamiento y soporte

Es frecuente que el centro de atención no tenga la capacidad de resolver en primera instancia un incidente, por lo que debe recurrir a un especialista o a algún superior que pueda tomar decisiones que escapan de su responsabilidad. A este proceso se le denomina escalar un incidente.

Básicamente hay dos formas de escalar incidentes:

- Funcional: Se requiere el apoyo de un especialista de más alto nivel para atender el incidente.
- Jerárquico: Se acude a un superior, de mayor autoridad, para tomar decisiones que escapan de las atribuciones del primer nivel, como por ejemplo, asignar más recursos para la atención de un incidente específico.

## **5.- Actividades**

Las actividades que se cumplen en el proceso de atención de incidentes son:

1. Registro de incidentes
2. Clasificación de los incidentes
3. Análisis, Resolución y Cierre de Incidentes

### **5.1.- Registro de incidentes**

La admisión y registro del incidente es el primer paso para una correcta gestión del mismo.

Los incidentes pueden provenir de diversas fuentes tales como usuarios, de la gestión de aplicaciones, del mismo centro atención o de soporte técnico, entre otros. Inmediatamente debe realizarse el proceso de registro, pues resulta mucho más costoso hacerlo posteriormente y se corre el riesgo de que la aparición de nuevos incidentes demore indefinidamente el proceso de registro.

En el proceso de registrar un incidente, se cumplen las siguientes tareas:

- Al realizarse la admisión del incidente en el centro de atención debe evaluarse en primera instancia si el servicio está incluido en los acuerdos de servicio establecidos con el usuario o el cliente. En caso de que no fuese así, el requerimiento deberá referirse a una autoridad competente.
- Debe comprobarse que el incidente no haya sido registrado, pues es común que varios usuarios notifiquen un mismo incidente.
- Debe asignarse un número de referencia al incidente, que lo identificará tanto para los procesos internos, como para las comunicaciones con el usuario o cliente.



- Se completará el registro inicial, introduciendo en la base de datos la información básica necesaria para la atención del incidente (hora, descripción del incidente, sistemas afectados...).
- Deberá incluirse cualquier información de apoyo que sea relevante para la resolución del incidente, que puede ser solicitada al cliente a través de un formulario específico, o que pueda ser obtenida de la propia base de datos de hardware y software.
- Se notificará el incidente a todos los usuarios que puedan resultar afectados por el incidente, con el fin de que conozcan cómo esta incidencia puede afectar su flujo normal de trabajo.

### **5.2.- Clasificación de los incidentes**

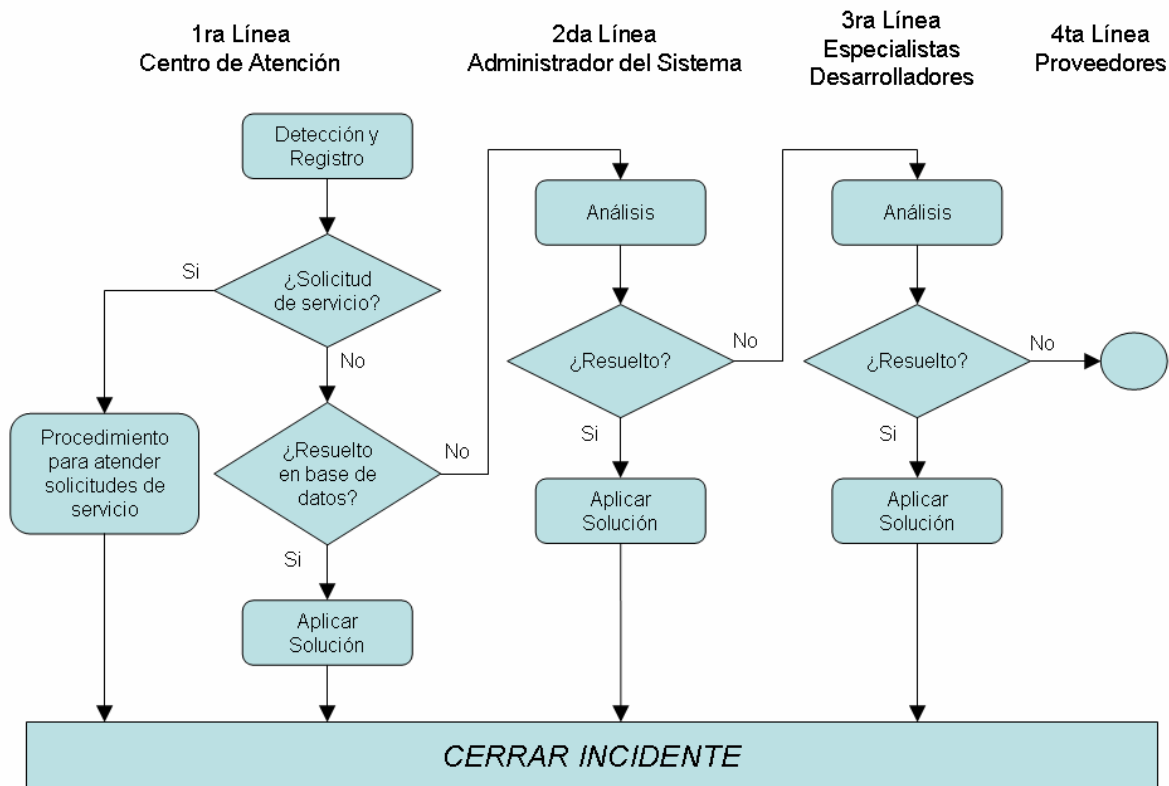
La clasificación de un incidente tiene como objetivo principal recopilar toda la información que pueda ser de utilidad para la resolución del mismo, para ello debe incluir las siguientes tareas:

- **Categorización:**  
La categorización de un incidente, como su nombre lo indica, consiste en la asignación de una categoría, dependiendo de los servicios afectados o del grupo de trabajo responsable de su resolución. La categoría de un incidente permite identificar los servicios afectados por el incidente.
- **Asignación de prioridad:**  
La asignación del nivel de prioridad, de acuerdo con el impacto y la urgencia y según los criterios que hayan sido preestablecidos.
- **Asignación de recursos:**  
En los casos en que el centro de atención no puede resolver el incidente en primera instancia, se deberá transferir al grupo de soporte técnico que corresponda y deberá designarse el personal que deberá atenderlo -segundo nivel-.
- **Seguimiento:**  
El supervisor del centro de atención hará seguimiento del progreso o estatus del incidente, así como del tiempo de respuesta esperado. Normalmente los estatus de un incidente pueden ser: registrado, en progreso, suspendido, escalado a nivel siguiente, resuelto y cerrado.

El tiempo de resolución del incidente corresponderá a los acuerdos de servicio que se hayan establecidos con los usuarios o clientes y a la prioridad que se haya asignado.

### 5.3.- *Análisis, Resolución y Cierre de Incidentes*

En primera instancia se examina el incidente con ayuda de la base de datos donde se acumulan y organizan las lecciones aprendidas –base de conocimiento-, para determinar si se puede identificar algún incidente ya resuelto y aplicar la solución ya conocida.



Si la resolución del incidente escapa a las posibilidades del centro de atención, éste lo transferirá a un segundo nivel, para su investigación por los expertos que se asignen. Si estos expertos logran atender el incidente se seguirán los procedimientos para escalar incidentes que se hayan preestablecido.

Durante todo el ciclo de vida del incidente se debe actualizar la información almacenada en las correspondientes bases de datos para que el personal involucrado en un incidente y su solución dispongan de información actualizada sobre el estatus del mismo -registrado, en progreso, suspendido, escalado a nivel siguiente, resuelto o cerrado-.

Existen casos en que para aplicar las medidas que permitan reanudar el servicio será necesario producir una solicitud de cambio, que normalmente corresponderá a un cambio urgente.

Cuando se haya solucionado un incidente se deberá:

- Cotejar con los usuarios que la solución ha sido satisfactoria.
- Incorporar las lecciones aprendidas en la base de conocimientos.
- Cerrar el incidente -colocarlo en estatus cerrado-.

## ***6.- Evaluación de la disciplina***

Para evaluar el desempeño de la disciplina de manejo de incidentes, será importante generar periódicamente diferentes reportes y generar información para otras disciplinas como:

- **Administración de Niveles de Servicio**  
Será fundamental que usuarios y los clientes dispongan de información puntual sobre el cumplimiento de los niveles de servicio acordados y de las medidas correctivas que deberán tomarse, en caso de incumplimiento.
- **Seguimiento del desempeño del centro de servicio**  
Para conocer el grado de satisfacción de los usuarios y clientes por el servicio prestado y supervisar el correcto funcionamiento de la primera línea de soporte.
- **Optimización de la asignación de recursos**  
Todos los administradores de servicios deben saber si los procedimientos para escalar incidentes se han cumplido adecuadamente y si se han evitado duplicidades en el proceso de atención de incidentes.
- **Identificación de deficiencias en los procedimientos**  
Sobre todo en sus etapas iniciales, los procedimientos podrían tener deficiencias que no les permitan adecuarse a la estructura de la organización o las necesidades de los usuarios o clientes, por lo que se deban tomar medidas para corregirlos.
- **Acumulación de Información Estadística**  
La información que se acumula en el proceso de manejo de incidentes puede ser utilizada para que la gerencia de

servicios de TI haga proyecciones sobre requerimientos de recursos, costos asociados al servicio, etc.

Para la evaluación del desempeño de la disciplina será necesario establecer diferentes métricas, tomando en cuenta variables como las siguientes:

- Número de incidentes por categorías y prioridades.
- Tiempos de resolución clasificados de acuerdo al impacto y a la urgencia de los incidentes.
- Porcentaje de incidentes, clasificados por impacto y prioridad, que han sido resueltos en primera instancia por el centro de atención.
- Costos asociados a la disciplina.
- Uso de los recursos disponibles en el centro de atención.
- Grado de satisfacción de usuarios y/o clientes, que puede determinarse mediante encuestas periódicas, que permitan cuantificar la percepción del usuario con respecto a los servicios recibidos.